

The h -critical number of finite abelian groups

Béla Bajnok

Department of Mathematics, Gettysburg College
Gettysburg, PA 17325-1486 USA
E-mail: bbajnok@gettysburg.edu

December 4, 2014

Abstract

For a finite abelian group G and a positive integer h , the unrestricted (resp. restricted) h -critical number $\chi(G, h)$ (resp. $\hat{\chi}(G, h)$) of G is defined to be the minimum value of m , if exists, for which the h -fold unrestricted (resp. restricted) sumset of every m -subset of G equals G itself. Here we determine $\chi(G, h)$ for all G and h ; and prove several results for $\hat{\chi}(G, h)$, including the cases of any G and $h = 2$, any G and large h , and any h for the cyclic group \mathbb{Z}_n of even order. We also provide a lower bound for $\hat{\chi}(\mathbb{Z}_n, 3)$ that we believe is exact for every n —this conjecture is a generalization of the one made by Gallardo, Grekos, et al. that was proved (for large n) by Lev.

2010 Mathematics Subject Classification:

Primary: 11B75;

Secondary: 05D99, 11B25, 11P70, 20K01.

Key words and phrases:

critical number, abelian groups, sumsets, restricted sumsets.

1 Introduction

Throughout this paper, G denotes a finite abelian group of order $n \geq 2$, written in additive notation. For a positive integer h and a nonempty subset A of G , we let hA and $\hat{h}A$ denote the h -fold *unrestricted sumset* and the h -fold *restricted sumset* of A , respectively; that is, hA is the collection of sums of h not-necessarily-distinct elements of A , and $\hat{h}A$ consists of all sums of h distinct elements of A . Furthermore, we set $\Sigma A = \cup_{h=0}^{\infty} \hat{h}A$.

The study of critical numbers originated with the 1964 paper [11] of Erdős and Heilbronn, in which they asked for the least integer m so that for every set A consisting of m nonzero elements of

the cyclic group \mathbb{Z}_p of prime order p , we have $\Sigma A = \mathbb{Z}_p$. More generally, one can define the *critical number* of G as

$$\chi^*(G) = \min\{m : A \subseteq G \setminus \{0\}, |A| \geq m \Rightarrow \Sigma A = G\}.$$

Here the $*$ indicates that only subsets of $G \setminus \{0\}$ are considered; alternately, some have studied

$$\chi(G) = \min\{m : A \subseteq G, |A| \geq m \Rightarrow \Sigma A = G\}.$$

It took nearly half a century, but now, due to the combined results of Diderrich and Mann [8], Diderrich [7], Mann and Wou [21], Dias Da Silva and Hamidoune [6], Gao and Hamidoune [15], Griggs [17], and Freeze, Gao, and Geroldinger [12, 13], we have the critical number of every group:

Theorem 1 (The combined results of authors above) *Suppose that $n \geq 10$, and let p be the smallest prime divisor of n . Then*

$$\chi^*(G) = \chi(G) - 1 = \begin{cases} \lfloor 2\sqrt{n-2} \rfloor & \text{if } G \text{ is cyclic of order } n = p \text{ or } n = pq \text{ where} \\ & q \text{ is prime and } 3 \leq p \leq q \leq p + \lfloor 2\sqrt{p-2} \rfloor + 1^1, \\ n/p + p - 2 & \text{otherwise.} \end{cases}$$

We note that considering unrestricted sums rather than restricted sums makes the problem trivial: the corresponding unrestricted critical numbers $\chi(G)$ and $\chi^*(G)$, using the notations of Theorem 1, are clearly given by

$$\chi^*(G) = \chi(G) - 1 = n/p.$$

We now turn to our present subject: the critical number when only a fixed number of terms are added. Here we consider both unrestricted sums and restricted sums; in particular, for a positive integer h , we define—if they exist, more on this below—the *unrestricted h -critical number* $\chi(G, h)$ and the *restricted h -critical number* $\chi^*(G, h)$ as the minimum values of m for which, respectively, the h -fold sumset and the h -fold restricted sumset of every m -element subset of G is G itself:

$$\chi(G, h) = \min\{m : A \subseteq G, |A| \geq m \Rightarrow hA = G\},$$

$$\chi^*(G, h) = \min\{m : A \subseteq G, |A| \geq m \Rightarrow h^*A = G\}.$$

It is easy to see that for all G and h we have $hG = G$, so $\chi(G, h)$ is always well defined; in Section 2 we determine that $\chi^*(G, h)$ is well defined if, and only if, one of the following holds:

- $h \in \{1, n-1\}$,
- $h \in \{2, n-2\}$, and G is not isomorphic to an elementary abelian 2-group,
- $3 \leq h \leq n-3$.

Furthermore, in Section 2 we explain that the versions

$$\chi^*(G, h) = \min\{m : A \subseteq G \setminus \{0\}, |A| \geq m \Rightarrow hA = G\}$$

¹Note that $\lfloor 2\sqrt{n-2} \rfloor = n/p + p - 1$ in this case.

and

$$\chi^*(G, h) = \min\{m : A \subseteq G \setminus \{0\}, |A| \geq m \Rightarrow hA = G\}$$

need not be studied separately, since—other than some trivial cases that we specify—they are well defined whenever their non-* versions are, and we have

$$\chi^*(G, h) = \chi(G, h)$$

and

$$\chi^*(G, h) = \chi(G, h).$$

So let us see what we can say about the quantities $\chi(G, h)$ and $\chi^*(G, h)$. We can determine the exact value of $\chi(G, h)$, as follows.

Recall that the minimum size

$$\rho(G, m, h) = \min\{|hA| : A \subseteq G, |A| = m\}$$

of h -fold sumsets of m -subsets of G is known for all G , m , and h . To state the result, we need the function

$$u(n, m, h) = \min\{f_d : d \in D(n)\},$$

where n , m , and h are positive integers, $D(n)$ is the set of positive divisors of n , and

$$f_d = (h \lceil m/d \rceil - h + 1) \cdot d.$$

(Here $u(n, m, h)$ is a relative of the Hopf–Stiefel function used also in topology and bilinear algebra; see, for example, [25], [23], and [19].) We then have:

Theorem 2 (Plagne; cf. [24]) *Let n , m , and h be positive integers with $m \leq n$. For any abelian group G of order n we have*

$$\rho(G, m, h) = u(n, m, h).$$

Theorem 2 allows us to determine $\chi(G, h)$; in order to do so, we introduce a—perhaps already familiar—function first.

Suppose that h and g are fixed positive integers; since we will only need the cases when $1 \leq g \leq h$, we make that assumption here. Recall that we let $D(n)$ denote the set of positive divisors of n . We then define

$$v_g(n, h) = \max \left\{ \left(\left\lfloor \frac{d-1-\gcd(d, g)}{h} \right\rfloor + 1 \right) \cdot \frac{n}{d} : d \in D(n) \right\}.$$

We should note that the function $v_g(n, h)$ has appeared elsewhere in additive combinatorics already. For example, according to the classical result of Diamanda and Yap (see [5]), the maximum size of a sum-free set (that is, a set A that is disjoint from $2A$) in the cyclic group \mathbb{Z}_n is given by

$$v_1(n, 3) = \begin{cases} \left(1 + \frac{1}{p}\right) \frac{n}{3} & \text{if } n \text{ has prime divisors congruent to } 2 \pmod{3}, \\ & \text{and } p \text{ is the smallest such divisor,} \\ \lfloor \frac{n}{3} \rfloor & \text{otherwise;} \end{cases}$$

similarly, this author proved (see [3]) that the maximum size of a $(3, 1)$ -sum-free set in \mathbb{Z}_n (where A is disjoint from $3A$) equals

$$v_2(n, 4) = \begin{cases} \left(1 + \frac{1}{p}\right) \frac{n}{4} & \text{if } n \text{ has prime divisors congruent to } 3 \bmod 4, \\ & \text{and } p \text{ is the smallest such divisor,} \\ \lfloor \frac{n}{4} \rfloor & \text{otherwise.} \end{cases}$$

It is believed that the analogous result for (k, l) -sum-free sets in \mathbb{Z}_n (where $kA \cap lA = \emptyset$ for positive integers $k > l$) is given by $v_{k-l}(n, k + l)$; this was established for the case when $k - l$ and n are relatively prime by Hamidoune and Plagne (see [18]). In Section 3 we provide a simpler alternate formula for $v_g(n, h)$, from which the expressions for $v_1(n, 3)$ and $v_2(n, 4)$ above will readily follow.

Returning now to the h -critical number of groups, in Section 4 we prove that for every group G of order n and for every h , we have

$$\chi(G, h) = v_1(n, h) + 1.$$

Evaluating the restricted h -critical number $\chi^{\wedge}(G, h)$ seems much more challenging, and this is, of course, due to the fact that we do not have a general formula for the minimum size

$$\rho^{\wedge}(G, m, h) = \min\{|hA| : A \subseteq G, |A| = m\}$$

of h -fold restricted sumsets of m -subsets of G . Indeed, we do not even know the value of $\rho^{\wedge}(G, m, h)$ for cyclic groups G and $h = 2$. Essentially the only general result is for groups of prime order; solving a conjecture made by Erdős and Heilbronn three decades earlier—not mentioned in [11] but in [10]—Dias Da Silva and Hamidoune succeeded in proving the following:

Theorem 3 (Dias Da Silva and Hamidoune; cf. [6]) *For a prime p and integers $1 \leq h \leq m \leq p$, we have*

$$\rho^{\wedge}(\mathbb{Z}_p, m, h) = \min\{p, hm - h^2 + 1\}.$$

(The result was reestablished, using different methods, by Alon, Nathanson, and Ruzsa; see [1], [2], and [22].) As a consequence, we have:

Corollary 4 *For any positive integer h and prime p with $h \leq p - 1$ we have*

$$\chi^{\wedge}(\mathbb{Z}_p, h) = \lfloor (p - 2)/h \rfloor + h + 1.$$

Let us see what else we can say about $\chi^{\wedge}(G, h)$. Trivially, for all groups G of order n we have

$$\chi^{\wedge}(G, 1) = \chi^{\wedge}(G, n - 1) = n.$$

In Section 5, we prove that for all G of order n and exponent at least 3, we have

$$\chi^{\wedge}(G, 2) = (n + |L|)/2 + 1,$$

where L denotes the subgroup of G that consists of elements of order at most 2. (Note that $n + |L|$ is always even; note also that for a group of exponent 2, $n = |L|$.) In particular, for $n \geq 3$ we have

$$\chi^{\wedge}(\mathbb{Z}_n, 2) = \lfloor n/2 \rfloor + 2.$$

As a consequence, we also show that this implies that if G has order n and exponent at least 3, and h is an integer with

$$(n + |L|)/2 - 1 \leq h \leq n - 2,$$

then

$$\chi^{\wedge}(G, h) = h + 2.$$

This leaves us with the task of determining $\chi^{\wedge}(G, h)$ for groups of composite order and

$$3 \leq h \leq (n + |L|)/2 - 2.$$

In Section 6 we complete this task for cyclic groups of even order; namely, we prove that for an even value of $n \geq 12$, we have

$$\chi^{\wedge}(\mathbb{Z}_n, h) = \begin{cases} n/2 + 1 & \text{if } 3 \leq h \leq n/2 - 2; \\ n/2 + 2 & \text{if } h = n/2 - 1. \end{cases}$$

(This result was established for $h = 3$ by Gallardo, Grekos, et al. in [14]; our proof for the general case is based on their method.)

In Section 7 we take a closer look at the case of $h = 3$. First, we prove tight lower bounds for $\chi^{\wedge}(\mathbb{Z}_n, 3)$ as $n \geq 11$. Namely, if n has prime divisors congruent to 2 mod 3 and p is the smallest such divisor, then we show that

$$\chi^{\wedge}(\mathbb{Z}_n, 3) \geq \begin{cases} \left(1 + \frac{1}{p}\right) \frac{n}{3} + 3 & \text{if } n = p \text{ or } n = 15, \\ \left(1 + \frac{1}{p}\right) \frac{n}{3} + 2 & \text{if } n = 3p \text{ with } p \neq 5, \\ \left(1 + \frac{1}{p}\right) \frac{n}{3} + 1 & \text{otherwise;} \end{cases}$$

and if n has no prime divisors congruent to 2 mod 3, then we prove that

$$\chi^{\wedge}(\mathbb{Z}_n, 3) \geq \begin{cases} \lfloor \frac{n}{3} \rfloor + 4 & \text{if } n \text{ is divisible by 9,} \\ \lfloor \frac{n}{3} \rfloor + 3 & \text{otherwise.} \end{cases}$$

We also claim that, actually, equality holds above for all n —this is certainly the case if n is even or prime; we have verified this (by computer) for all $n \leq 50$; and in Section 7 we prove that equality follows from a conjecture that appeared in [4]. Our conjecture is a generalization of the one made by Gallardo, Grekos, et al. in [14] that was proved (for large n) by Lev in [20].

The pursuit of finding the value of $\chi^{\wedge}(G, h)$ in general remains challenging and exciting.

2 Preliminary results

In this section we establish the conditions under which the four quantities $\chi(G, h)$, $\chi^{\wedge}(G, h)$, $\chi^*(G, h)$, and $\chi^{\wedge*}(G, h)$ exist; furthermore, we show that, when they exist, then

$$\chi(G, h) = \chi^*(G, h)$$

and

$$\chi(G, h) = \chi^*(G, h).$$

We start with the following easy result:

Proposition 5 *Let A be an m -subset of G and h be a positive integer.*

1. *If either*

(a) *$h = 1$ or*

(b) *A is a coset of a subgroup of G ,*

then $|hA| = m$.

2. *In all other cases, $|hA| \geq m + 1$.*

Proof: The first claim is trivial. To prove the second claim, we assume that $h \geq 2$ and that $|hA| \leq |A| = m$. We will show that for any $a \in A$, we have $A = a + H$, where H is the stabilizer subgroup of $(h - 1)A$; that is,

$$H = \{g \in G \mid g + (h - 1)A = (h - 1)A\}.$$

Consider the set $A' = A - a$. Then $|A'| = m$ and $0 \in A'$, and therefore

$$(h - 1)A = \{0\} + (h - 1)A \subseteq A' + (h - 1)A.$$

But then

$$|hA| = |hA - a| = |A' + (h - 1)A| \geq |(h - 1)A| \geq |(h - 2) \cdot a + A| = |A|;$$

since we assumed $|hA| \leq |A|$, equality must hold throughout, and thus

$$A' + (h - 1)A = (h - 1)A.$$

Therefore, $A' \subseteq H$, and so $A \subseteq a + H$, which implies that

$$|a + H| \geq |A| \geq |hA| = |(h - 1)A + A| \geq |(h - 1)A| = |H + (h - 1)A| \geq |H| = |a + H|.$$

Then equality must hold throughout, and thus $a + H = A$, establishing our claim. \square

As an immediate corollary, we see that $\chi(G, h)$ is well defined for all G and h , and $\chi^*(G, h)$ is well defined if, and only if, the trivial conditions $n \geq 3$ and $h \geq 2$ hold.

The version of Proposition 5 for restricted sumsets is substantially more complicated:

Theorem 6 (Girard, Griffiths, and Hamidoune; cf. [16]) *Let A be an m -subset of G , and suppose that $1 \leq h \leq m - 1$. We let L denote the subgroup of G that consists of elements of order at most 2.*

1. *If $h \in \{2, m - 2\}$ and A is a coset of a subgroup of L , then $|hA| = m - 1$.*

2. If any of the conditions

- (a) $h \in \{1, m-1\}$,
- (b) A is a coset of a subgroup of G ,
- (c) $h \in \{2, m-2\}$ and A consists of all but one element of a coset of a subgroup of L , or
- (d) $h \in \{2, m-2\}$ and $m = 4$ and A consists of two cosets of a subgroup of order 2

holds, then $|hA| = m$.

3. In all other cases, $|hA| \geq m+1$.

As a consequence, we get that $\chi^{\wedge}(G, h)$ is well defined if, and only if, one of the following holds:

- $h \in \{1, n-1\}$,
- $h \in \{2, n-2\}$, and G is not isomorphic to an elementary abelian 2-group,
- $3 \leq h \leq n-3$;

and $\chi^*(G, h)$ is well defined if, and only if, one of the following holds:

- $n = 5$ and $h = 2$,
- $n \geq 6$, $h \in \{2, n-2\}$, and G is not isomorphic to an elementary abelian 2-group;
- $3 \leq h \leq n-3$.

From this we can conclude that, other than the trivial cases of $h \in \{1, n-1\}$ or $n \leq 5$, $\chi^*(G, h)$ is well defined exactly when $\chi^{\wedge}(G, h)$ is.

Next we prove that our $*$ quantities are equal to their respective non- $*$ versions:

Proposition 7 *When they are defined, we have*

$$\chi^*(G, h) = \chi(G, h)$$

and

$$\chi^{\wedge}(G, h) = \chi^{\wedge}(G, h).$$

Proof: We only prove the first claim as the other is similar. For that, the other direction being obvious, we just need to show that

$$\chi^*(G, h) \geq \chi(G, h).$$

To see this, let B be a subset of G of size $\chi(G, h) - 1$ for which $hB \neq G$. Since $|B| \leq n-1$, we have $|-B| \leq n-1$ as well; let $g \in G \setminus (-B)$. Then $A = g + B$ has size $\chi(G, h) - 1$, and $A \subseteq G \setminus \{0\}$, since $0 \in A$ would contradict $g \notin -B$. But hA and hB have the same size, so we conclude that $hA \neq G$, from which our inequality follows. \square

To summarize this section: it suffices to study $\chi(G, h)$ and $\chi^{\wedge}(G, h)$.

3 The function $v_g(n, h)$

In this section we prove a result that greatly simplifies the evaluation of the function $v_g(n, h)$ that we defined in the Introduction.

Theorem 8 *Suppose that n, h , and g are positive integers and that $1 \leq g \leq h$. For $i = 2, 3, \dots, h-1$, let $P_i(n)$ be the set of those prime divisors of n that do not divide g and that leave a remainder of i when divided by h ; that is,*

$$P_i(n) = \{ p \in D(n) \setminus D(g) : p \text{ prime and } p \equiv i \pmod{h} \}.$$

We let I denote those values of $i = 2, 3, \dots, h-1$ for which $P_i(n) \neq \emptyset$, and for each $i \in I$, we let p_i be the smallest element of $P_i(n)$.

Then, the value of $v_g(n, h)$ is

$$v_g(n, h) = \begin{cases} \frac{n}{h} \cdot \max \left\{ 1 + \frac{h-i}{p_i} : i \in I \right\} & \text{if } I \neq \emptyset; \\ \left\lfloor \frac{n}{h} \right\rfloor & \text{if } I = \emptyset \text{ and } g \neq h; \\ \left\lfloor \frac{n-1}{h} \right\rfloor & \text{if } I = \emptyset \text{ and } g = h. \end{cases}$$

Proof: Suppose that d is a positive divisor of n , and define the function

$$f(d) = \left(\left\lfloor \frac{d-1-\gcd(d, g)}{h} \right\rfloor + 1 \right) \cdot \frac{n}{d}.$$

We first prove the following.

Claim 1: Let i be the remainder of d when divided by h . We then have

$$f(d) = \begin{cases} \frac{n}{h} \cdot \left(1 + \frac{h-i}{d} \right) & \text{if } \gcd(d, g) < i; \\ \frac{n}{h} \cdot \left(1 - \frac{h}{d} \right) & \text{if } h|d \text{ and } g = h; \\ \frac{n}{h} \cdot \left(1 - \frac{i}{d} \right) & \text{otherwise.} \end{cases}$$

Proof of Claim 1. We start with

$$\left\lfloor \frac{d-1-\gcd(d, g)}{h} \right\rfloor = \frac{d-i}{h} + \left\lfloor \frac{i-1-\gcd(d, g)}{h} \right\rfloor.$$

We investigate the maximum and minimum values of the quantity $\left\lfloor \frac{i-1-\gcd(d, g)}{h} \right\rfloor$.

For the maximum, we have

$$\left\lfloor \frac{i-1-\gcd(d, g)}{h} \right\rfloor \leq \left\lfloor \frac{(h-1)-1-1}{h} \right\rfloor \leq 0,$$

with equality if, and only if, $i - 1 - \gcd(d, g) \geq 0$; that is, $\gcd(d, g) < i$.

For the minimum, we get

$$\left\lfloor \frac{i - 1 - \gcd(d, g)}{h} \right\rfloor \geq \left\lfloor \frac{0 - 1 - g}{h} \right\rfloor \geq \left\lfloor \frac{0 - 1 - h}{h} \right\rfloor = -2,$$

with equality if, and only if, $i = 0$, $\gcd(d, g) = g$, and $g = h$; that is, $h|d$ and $g = h$.

The proof of Claim 1 now follows easily. \square

Claim 2: Using the notations as above, assume that $\gcd(d, g) \geq i$. Then

$$f(d) \leq \begin{cases} \frac{n}{h} & \text{if } g \neq h; \\ \frac{n-1}{h} & \text{if } g = h. \end{cases}$$

Proof of Claim 2. By Claim 1, we have

$$f(d) \leq \frac{n}{h}.$$

Furthermore, unless $i = 0$ and $g \neq h$, we have

$$f(d) \leq \frac{n}{h} \cdot \left(1 - \frac{1}{d}\right) \leq \frac{n}{h} \cdot \left(1 - \frac{1}{n}\right) = \frac{n-1}{h}.$$

\square

Claim 3: For all g , h , and n we have

$$v_g(n, h) \geq \begin{cases} \left\lfloor \frac{n}{h} \right\rfloor & \text{if } g \neq h; \\ \left\lfloor \frac{n-1}{h} \right\rfloor & \text{if } g = h. \end{cases}$$

Proof of Claim 3. We first note that

$$\begin{aligned} v_g(n, h) &= \max \left\{ \left(\left\lfloor \frac{d-1-\gcd(d, g)}{h} \right\rfloor + 1 \right) \cdot \frac{n}{d} : d \in D(n) \right\} \\ &\geq \left\lfloor \frac{n-1-\gcd(n, g)}{h} \right\rfloor + 1 \\ &\geq \left\lfloor \frac{n-1-g}{h} \right\rfloor + 1. \end{aligned}$$

The claim now follows, since $g+1 \leq h$, unless $g = h$ in which case

$$\left\lfloor \frac{n-1-g}{h} \right\rfloor + 1 = \left\lfloor \frac{n-1}{h} \right\rfloor.$$

\square

We are now ready for the proof of Theorem 8.

Proof of Theorem 8. Let d_0 be any positive divisor of n for which $v_g(n, h) = f(d_0)$; let i_0 be the remainder of $d_0 \bmod h$. The following two claims together establish Theorem 8.

Claim 4: If $\gcd(d_0, g) \geq i_0$, then $I = \emptyset$ and

$$v_g(n, h) = \begin{cases} \lfloor \frac{n}{h} \rfloor & \text{if } g \neq h; \\ \lfloor \frac{n-1}{h} \rfloor & \text{if } g = h \end{cases}$$

Proof of Claim 4: By Claim 2,

$$v_g(n, h) = f(d_0) \leq n/h.$$

If we were to have an element $i \in I$, then for the corresponding prime divisor p_i of n we have

$$\gcd(p_i, g) = 1 < i,$$

thus by Claim 1,

$$v_g(n, h) \geq f(p_i) = \frac{n}{h} \cdot \left(1 + \frac{h-i}{p_i}\right) > \frac{n}{h},$$

a contradiction. The result now follows from Claims 2 and 3. \square

Claim 5: If $\gcd(d_0, g) < i_0$, then $i_0 \in I$, $d_0 \in P_{i_0}(n)$, and

$$v_g(n, h) = \frac{n}{h} \cdot \left(1 + \frac{h-i_0}{d_0}\right).$$

Proof of Claim 5: First, we prove that d_0 is prime. Note that our assumption implies that $i_0 \geq 2$, and thus d_0 has no divisor that is divisible by h , and has at least one prime divisor that leaves a remainder greater than 1 mod h . Let p be the smallest prime divisor of d_0 that leaves a remainder more than 1 mod h , and let i be this remainder.

We establish the inequality

$$\frac{h-2}{p^2} < \frac{h-i}{p},$$

as follows. Since $i \leq h-1$, the inequality clearly holds when $p > h-2$, so let us assume that $p \leq h-2$. Note that, in this case, $i = p$, so we need to establish that

$$\frac{h-2}{p^2} < \frac{h-p}{p};$$

this is not hard either since we have

$$h-2 = hp - h(p-1) - 2 \leq hp - (p+2)(p-1) - 2 = hp - p^2 - p < (h-p)p.$$

Assume now that $i \neq i_0$, and thus $d_0/p \not\equiv 1 \pmod{h}$. Then d_0/p also has a prime divisor, say p' , that leaves a remainder greater than 1 mod h , and by the choice of p , $p' \geq p$ and thus $d_0 \geq p^2$. But then we have

$$v_g(n, h) = f(d_0) = \frac{n}{h} \cdot \left(1 + \frac{h-i_0}{d_0}\right) \leq \frac{n}{h} \cdot \left(1 + \frac{h-2}{p^2}\right) < \frac{n}{h} \cdot \left(1 + \frac{h-i}{p}\right) = f(p),$$

a contradiction.

Therefore, $i = i_0$, and thus

$$v_g(n, h) = f(d_0) = \frac{n}{h} \cdot \left(1 + \frac{h - i_0}{d_0}\right) \leq \frac{n}{h} \cdot \left(1 + \frac{h - i_0}{p}\right) = f(p);$$

since we must have equality, $d_0 = p$ follows.

This establishes the fact that d_0 is prime. Since

$$\gcd(d_0, g) < i_0 \leq d_0,$$

d_0 cannot divide g . This establishes Claim 5, and thus completes the proof of Theorem 8. \square

We should also note that it is easy to show that, when $I \neq \emptyset$ in the statement of Theorem 8, there is a unique i (and thus p_i) for which $\frac{h-i}{p_i}$ is maximal.

4 The unrestricted h -critical number

Recall from our Introduction that

$$v_1(n, h) = \max \left\{ \left(\left\lfloor \frac{d-2}{h} \right\rfloor + 1 \right) \cdot \frac{n}{d} : d \in D(n) \right\}.$$

Here we prove the following:

Theorem 9 *For all finite abelian groups G of order n and all positive integers h , the (unrestricted) h -critical number of G equals*

$$\chi(G, h) = v_1(n, h) + 1.$$

Proof: We need to prove that, for $m = v_1(n, h)$, we have

$$u(n, m, h) < n$$

but

$$u(n, m+1, h) \geq n.$$

Let $d_0 \in D(n)$ be such that

$$v_1(n, h) = \max \left\{ \left(\left\lfloor \frac{d-2}{h} \right\rfloor + 1 \right) \cdot \frac{n}{d} : d \in D(n) \right\} = \left(\left\lfloor \frac{d_0-2}{h} \right\rfloor + 1 \right) \cdot \frac{n}{d_0}.$$

To establish the first inequality, simply note that $u(n, m, h) \leq f_{n/d_0}(m, h)$ where

$$f_{n/d_0}(m, h) = \left(h \cdot \left(\left\lfloor \frac{d_0-2}{h} \right\rfloor + 1 \right) - h + 1 \right) \cdot \frac{n}{d_0} = \left(h \cdot \left\lfloor \frac{d_0-2}{h} \right\rfloor + 1 \right) \cdot \frac{n}{d_0} \leq (d_0 - 1) \cdot \frac{n}{d_0} < n.$$

For the second inequality, we must prove that, for any $d \in D(n)$, we have $f_d(m+1, h) \geq n$; that is,

$$h \cdot \left\lceil \frac{\left(\left\lfloor \frac{d_0-2}{h} \right\rfloor + 1\right) \cdot \frac{n}{d_0} + 1}{d} \right\rceil - h + 1 \geq \frac{n}{d}.$$

But $n/d \in D(n)$, so by the choice of d_0 , we have

$$\left(\left\lfloor \frac{d_0-2}{h} \right\rfloor + 1\right) \cdot \frac{n}{d_0} \geq \left(\left\lfloor \frac{n/d-2}{h} \right\rfloor + 1\right) \cdot \frac{n}{n/d},$$

and thus

$$\begin{aligned} h \cdot \left\lceil \frac{\left(\left\lfloor \frac{d_0-2}{h} \right\rfloor + 1\right) \cdot \frac{n}{d_0} + 1}{d} \right\rceil - h + 1 &\geq h \cdot \left\lceil \left(\left\lfloor \frac{n/d-2}{h} \right\rfloor + 1\right) + \frac{1}{d} \right\rceil - h + 1 \\ &= h \cdot \left(\left\lfloor \frac{n/d-2}{h} \right\rfloor + 2\right) - h + 1 \\ &\geq h \cdot \left(\frac{n/d-2-(h-1)}{h} + 2\right) - h + 1 \\ &= \frac{n}{d}. \end{aligned}$$

Our proof is complete. \square

5 The restricted h -critical number for $h = 2$ and large h

First, we evaluate $\chi^{\wedge}(G, 2)$:

Proposition 10 *Suppose that G is of order n and is not isomorphic to the elementary abelian 2-group, and let L denote its subset—indeed, subgroup—consisting of elements of order at most 2. Then*

$$\chi^{\wedge}(G, 2) = (n + |L|)/2 + 1.$$

In particular, for $n \geq 3$ we have

$$\chi^{\wedge}(\mathbb{Z}_n, 2) = \lfloor n/2 \rfloor + 2.$$

We first prove the following.

Lemma 11 *For a given $g \in G$, let $L_g = \{x \in G \mid 2x = g\}$. If $L_g \neq \emptyset$, then $|L_g| = |L|$.*

Proof: Choose an element $x \in L_g$. Then $x - L_g \subseteq L$, so $|x - L_g| = |L_g| \leq |L|$.

Similarly, $x + L \subseteq L_g$, so $|x + L| = |L| \leq |L_g|$. \square

Proof of Proposition 10: Suppose first that

$$m = (n + |L|)/2 + 1.$$

Note that our assumption on G implies that $3 \leq m \leq n$.

Let A be an m -subset of G , let $g \in G$ be arbitrary, and set $B = g - A$. Then $|B| = m$, and thus

$$|A \cap B| = |A| + |B| - |A \cup B| \geq 2m - n = |L| + 2.$$

By our lemma above, we must have an element $a_1 \in A \cap B$ for which $a_1 \notin L_g$. Since $a_1 \in A \cap B$, we also have an element $a_2 \in A$ for which $a_1 = g - a_2$ and thus $g = a_1 + a_2$. But $a_1 \notin L_g$, and therefore $a_2 \neq a_1$. In other words, $g \in 2^{\wedge}A$; since g was arbitrary, we have $G = 2^{\wedge}A$, as claimed.

For the other direction, we need to find a subset A of G with

$$|A| = (n + |L|)/2$$

for which $2^{\wedge}A \neq G$. Observe that the elements of $G \setminus L$ are distinct from their inverses, so we have a (possibly empty) subset K of $G \setminus L$ with which

$$G = L \cup K \cup (-K),$$

and L , K , and $-K$ are pairwise disjoint. Now set $A = L \cup K$. Clearly, A has the right size; furthermore, it is easy to verify that $0 \notin 2^{\wedge}A$ and thus $2^{\wedge}A \neq G$. \square

Next, we show how Proposition 10 allows us evaluate $\chi^{\wedge}(G, h)$ for all large values of h . In particular, we have:

Proposition 12 *Suppose that G is not an elementary abelian 2-group and h is a positive integer with*

$$(n + |L|)/2 - 1 \leq h \leq n - 2.$$

Then

$$\chi^{\wedge}(G, h) = h + 2.$$

Proof: Assume first that A is an $(h + 1)$ -subset of G . Then

$$|h^{\wedge}A| = h + 1 \leq n - 1,$$

so $\chi^{\wedge}(G, h)$ is at least $h + 2$.

Now let A be an $(h + 2)$ -subset of G . Then, by symmetry, $|h^{\wedge}A| = |2^{\wedge}A|$; since

$$|A| = h + 2 \geq (n + |L|)/2 + 1,$$

by Proposition 10 we have $h^{\wedge}A = G$. This establishes our claim. \square

6 The restricted h -critical number of cyclic groups of even order

Here we determine the value of $\chi^{\wedge}(\mathbb{Z}_n, h)$ for all values of h when n is even:

Theorem 13 Suppose that n is even and $n \geq 12$. Then

$$\chi^{\wedge}(\mathbb{Z}_n, h) = \begin{cases} n & \text{if } h = 1; \\ n/2 + 2 & \text{if } h = 2; \\ n/2 + 1 & \text{if } h = 3, 4, \dots, n/2 - 2; \\ n/2 + 2 & \text{if } h = n/2 - 1; \\ h + 2 & \text{if } h = n/2, n/2 + 1, \dots, n - 2; \\ n & \text{if } h = n - 1. \end{cases}$$

Theorem 13 was established for $h = 3$ by Gallardo, Grekos, et al. in [14]; our proof for the general case is based on their method as well as Theorem 6 above.

Proof: The cases of $h \leq 2$ or $h \geq n/2$ have been already addressed, leaving only $3 \leq h \leq n/2 - 1$. In fact, as we now show, it suffices to treat the cases of $3 \leq h \leq n/4$:

To conclude that we then have $\chi^{\wedge}(\mathbb{Z}_n, h) = n/2 + 1$ for

$$n/4 + 1 \leq h \leq n/2 - 2$$

as well, note that, obviously, $\chi^{\wedge}(\mathbb{Z}_n, h) \geq n/2 + 1$, and that if A is a subset of \mathbb{Z}_n of size $n/2 + 1$, then, since

$$3 \leq n/2 + 1 - h \leq n/4,$$

we have

$$|h^{\wedge}A| = |(n/2 + 1 - h)^{\wedge}A| = n.$$

Similarly, with $\chi^{\wedge}(\mathbb{Z}_n, 2) = n/2 + 2$ and $\chi^{\wedge}(\mathbb{Z}_n, 3) = n/2 + 1$ we can settle the case of $h = n/2 - 1$: Choosing a subset A of \mathbb{Z}_n of size $n/2 + 1$ for which $|2^{\wedge}A| < n$ implies that we also have

$$|(n/2 - 1)^{\wedge}A| < n$$

and thus $\chi^{\wedge}(\mathbb{Z}_n, n/2 - 1)$ is at least $n/2 + 2$; while for any $B \subset \mathbb{Z}_n$ of size $n/2 + 2$ we get

$$|(n/2 - 1)^{\wedge}B| = |3^{\wedge}B| = n.$$

Therefore, for the rest of the proof, we assume that $3 \leq h \leq n/4$.

Since we clearly have $\chi^{\wedge}(\mathbb{Z}_n, h) \geq n/2 + 1$, it suffices to prove the reverse inequality. For that, let A be a subset of \mathbb{Z}_n of size $n/2 + 1$; we need to prove that $h^{\wedge}A = \mathbb{Z}_n$.

Let O and E denote the set of odd and even elements of \mathbb{Z}_n , respectively, and let A_O and A_E be the set of odd and even elements of A , respectively. Note that both A_O and A_E have size at most $n/2$ and thus neither can be empty. We will consider four cases:

Assume first that $|A_O| \leq 2$. Then $|A_E| \geq n/2 - 1$. Observe that $3 \leq h \leq n/4$ and $n \geq 12$ imply that

$$2 \leq h - 1 < h \leq n/2 - 3,$$

and $n/2 - 1$ is not a divisor of n . Therefore, by Theorem 6, both $(h-1)\hat{A}_E$ and $h\hat{A}_E$ have size at least $n/2$. But, of course, both $(h-1)\hat{A}_E$ and $h\hat{A}_E$ are subsets of E , so

$$(h-1)\hat{A}_E = h\hat{A}_E = E.$$

Now let a be any element of A_O ; we then see that

$$a + (h-1)\hat{A}_E = a + E = O.$$

Therefore,

$$(a + (h-1)\hat{A}_E) \cup h\hat{A}_E = O \cup E = \mathbb{Z}_n;$$

since both $a + (h-1)\hat{A}_E$ and $h\hat{A}_E$ are subsets of $h\hat{A}$, we get $h\hat{A} = \mathbb{Z}_n$.

Next, we assume that $|A_E| \leq 2$. In this case, an argument similar to the one in the previous case yields that

$$(h-1)\hat{A}_O = \begin{cases} O & \text{if } h \text{ is even,} \\ E & \text{if } h \text{ is odd;} \end{cases}$$

and

$$h\hat{A}_O = \begin{cases} E & \text{if } h \text{ is even,} \\ O & \text{if } h \text{ is odd.} \end{cases}$$

Let a be any element of A_E ; we get

$$(a + (h-1)\hat{A}_O) \cup h\hat{A}_O = \mathbb{Z}_n$$

regardless of whether h is even or odd; therefore, $h\hat{A} = \mathbb{Z}_n$.

Before turning to the last two cases, we observe that, since $h \leq n/4$, we have

$$|A| = n/2 + 1 \geq 2h + 1,$$

and thus at least one of A_O or A_E must have size at least $h + 1$.

Consider the case when $|A_O| \geq 3$ and $|A_E| \geq h + 1$. Referring to Theorem 6 again, we deduce that $(h-2)\hat{A}_E$ and $(h-1)\hat{A}_E$ both have size at least $|A_E|$, and that $2\hat{A}_O$ is of size at least $|A_O|$.

Now let g_O be any element of O ; we have

$$|g_O - A_O| + |(h-1)\hat{A}_E| \geq |A_O| + |A_E| = n/2 + 1.$$

But $g_O - A_O$ and $(h-1)\hat{A}_E$ are both subsets of E , so they cannot be disjoint; this then means that g_O can be written as the sum of an element of A_O and $h-1$ distinct elements of A_E , so $g_O \in h\hat{A}$.

Similarly, for any element g_E of E , we have

$$|g_E - (h-2)\hat{A}_E| + |2\hat{A}_O| \geq |A_E| + |A_O| = n/2 + 1,$$

and thus g_E can be written as the sum of $h-2$ distinct elements of A_E and two distinct elements of A_O , so $g_E \in h\hat{A}$.

Combining the last two paragraphs yields $O \cup E \subseteq h\hat{A}$ and thus $h\hat{A} = \mathbb{Z}_n$.

For our fourth case, assume that $|A_E| \geq 3$ and $|A_O| \geq h + 1$. As above, we can conclude that $|(h-2)\hat{A}_O| \geq |A_O|$, $|(h-1)\hat{A}_O| \geq |A_O|$, and $|2\hat{A}_E| \geq |A_E|$.

Let g be any element of \mathbb{Z}_n . If g and h are of the same parity (both even or both odd), then we find that $g - (h - 2)A_O$ and $2A_E$ are each subsets of E . As above, we see that they cannot be disjoint, and thus

$$g \in (h - 2)A_O + 2A_E \subseteq hA.$$

The subcase when g is even and h is odd is similar: this time we see that $g - (h - 1)A_O$ and A_E are each subsets of E and that they cannot be disjoint, so

$$g \in (h - 1)A_O + A_E \subseteq hA.$$

The final subcase, when g is odd and h is even, needs more work. We first prove that there is at most one element $a \in A_O$ for which $A_O \setminus \{a\}$ is the coset of a subgroup of \mathbb{Z}_n . Suppose, indirectly, that a_1 and a_2 are distinct elements of A_O so that $A_O \setminus \{a_1\}$ and $A_O \setminus \{a_2\}$ are both cosets. In this case, they must be cosets of the same subgroup since \mathbb{Z}_n has only one subgroup of that size. But $|A_O| \geq 3$, so $A_O \setminus \{a_1\}$ and $A_O \setminus \{a_2\}$ are not disjoint, which implies that they are actually equal, which is a contradiction since a_1 is an element of $A_O \setminus \{a_2\}$ but not of $A_O \setminus \{a_1\}$.

We also need to consider the special case when $|A_O| = 5$; we can then see that there is at most one element $a \in A_O$ for which $A_O \setminus \{a\}$ is the union of two cosets of $\{0, n/2\}$.

Hence we have an element $a_O \in A_O$ so that $A_O \setminus \{a_O\}$ is not the coset of a subgroup of \mathbb{Z}_n , and not the union of two cosets of the subgroup of size 2. But then, by Theorem 6,

$$|(h - 2)(A_O \setminus \{a_O\})| \geq |A_O|.$$

Therefore,

$$|(h - 2)(A_O \setminus \{a_O\})| + |g - a_O - A_E| \geq |A_O| + |A_E| = n/2 + 1;$$

since both $(h - 2)(A_O \setminus \{a_O\})$ and $g - a_O - A_E$ are subsets of E , this can only happen if they are not disjoint, which means that

$$g \in (h - 2)(A_O \setminus \{a_O\}) + (a_O + A_E) \subseteq hA.$$

This completes our proof. \square

7 The restricted 3-critical number of cyclic groups

In this section we summarize what we can say about the case of $h = 3$ in the cyclic group of order n .

We will rely on the following result:

Theorem 14 (B.; cf. [4]) *For all positive integers n and m with $4 \leq m \leq n$ we have*

$$\rho^\wedge(\mathbb{Z}_n, m, 3) \leq \begin{cases} \min\{u(n, m, 3), 3m - 3 - \gcd(n, m - 1)\} & \text{if } \gcd(n, m - 1) \geq 8; \\ \min\{u(n, m, 3), 3m - 10\} & \text{if } \gcd(n, m - 1) = 7, \text{ or} \\ & \gcd(n, m - 1) \leq 5, 3|n, \text{ and } 3|m, \text{ or} \\ & \gcd(n, m - 1) \leq 5, (3m - 9)|n, \text{ and } 5|(m - 3); \\ \min\{u(n, m, 3), 3m - 9\} & \text{if } \gcd(n, m - 1) = 6, \text{ or} \\ & m = 6 \text{ and } 10|n \text{ but } 3 \nmid n; \\ \min\{u(n, m, 3), 3m - 8\} & \text{otherwise.} \end{cases}$$

Our result for $\chi^\wedge(\mathbb{Z}_n, 3)$ is, as follows:

Proposition 15 *Let n be an arbitrary integer with $n \geq 11$.*

1. *If n has prime divisors congruent to 2 mod 3 and p is the smallest such divisor, then*

$$\chi^\wedge(\mathbb{Z}_n, 3) \geq \begin{cases} \left(1 + \frac{1}{p}\right) \frac{n}{3} + 3 & \text{if } n = p \text{ or } n = 15; \\ \left(1 + \frac{1}{p}\right) \frac{n}{3} + 2 & \text{if } n = 3p \text{ with } p \neq 5; \\ \left(1 + \frac{1}{p}\right) \frac{n}{3} + 1 & \text{otherwise.} \end{cases}$$

2. *If n has no prime divisors congruent to 2 mod 3, then*

$$\chi^\wedge(\mathbb{Z}_n, 3) \geq \begin{cases} \left\lfloor \frac{n}{3} \right\rfloor + 4 & \text{if } n \text{ is divisible by 9;} \\ \left\lfloor \frac{n}{3} \right\rfloor + 3 & \text{otherwise.} \end{cases}$$

Proof: Note that the case when n is even follows from Theorem 13, since

$$\left(1 + \frac{1}{2}\right) \frac{n}{3} + 1 = \frac{n}{2} + 1;$$

and the case when n is prime follows from Theorem 4 since

$$\left\lfloor \frac{p-2}{3} \right\rfloor + 3 + 1 = \begin{cases} \left(1 + \frac{1}{p}\right) \frac{p}{3} + 3 & \text{if } p \equiv 2 \pmod{3}; \\ \left\lfloor \frac{p}{3} \right\rfloor + 3 & \text{otherwise.} \end{cases}$$

Therefore, we may assume that n is odd and composite. The case of $n = 15$ can be computed individually, so we also assume that $n \geq 21$.

We observe first that for

$$m = \left\lfloor \frac{n}{3} \right\rfloor + 2$$

we have

$$\rho^{\wedge}(\mathbb{Z}_n, m, 3) \leq u^{\wedge}(n, m, 3) \leq 3m - 8 \leq n - 2,$$

so we always have

$$\chi^{\wedge}(\mathbb{Z}_n, 3) \geq \left\lfloor \frac{n}{3} \right\rfloor + 3.$$

Assume now that n has no prime divisors congruent to 2 mod 3 and that n is divisible by 9; let $m = n/3 + 3$. Then $m - 1$ and n are relatively prime, since if d is a divisor of both $m - 1$ and n , then d will divide both $3m - 3$ and n , and hence also their difference, which is 6. However, n is odd and $m - 1$ is not divisible by 3 (since m is), so $d = 1$. According to Theorem 14,

$$\rho^{\wedge}(\mathbb{Z}_n, m, 3) \leq \min\{u(n, m, 3), 3m - 10\} \leq 3m - 10 = n - 1,$$

so $\chi^{\wedge}(\mathbb{Z}_n, 3) \geq n/3 + 4$.

Suppose now that n has a prime divisors congruent to 2 mod 3, and let p be the smallest of these. We then have

$$\chi^{\wedge}(\mathbb{Z}_n, 3) \geq \chi(\mathbb{Z}_n, 3) = v_1(n, 3) + 1 = \left(1 + \frac{1}{p}\right) \frac{n}{3} + 1.$$

Now if $n = 3p$, then we further have

$$\chi^{\wedge}(\mathbb{Z}_n, 3) \geq \left(1 + \frac{1}{p}\right) \frac{n}{3} + 2,$$

since for

$$m = \left(1 + \frac{1}{p}\right) \frac{n}{3} + 1 = p + 2$$

we have

$$\rho^{\wedge}(\mathbb{Z}_n, m, 3) \leq u^{\wedge}(n, m, 3) \leq 3m - 8 = 3p - 2 = n - 2.$$

Our proof is now complete. \square

In [4] we made the following conjecture:

Conjecture 16 *For all n and m , we have equality in Theorem 14.*

Correspondingly, we believe that:

Conjecture 17 *For all values of $n \geq 11$, equality holds in Proposition 15.*

We have verified that Conjecture 17 holds for all values of $n \leq 50$, and by Theorems 4 and 13, it holds when n is prime or even. As additional support, we prove the following:

Theorem 18 *Conjecture 16 implies Conjecture 17.*

Proof: As we noted before, we may assume that n is odd, composite, and greater than 15.

Suppose first that n has a prime divisor that is congruent to 2 mod 3, and let p be the smallest such prime; since n is odd, $p \geq 5$. Let us set

$$m = \left(1 + \frac{1}{p}\right) \frac{n}{3} + 1.$$

We need to prove that Conjecture 16 implies both of the following statements:

A: $\rho^{\wedge}(\mathbb{Z}_n, m+1, 3) = n$.

B: If $\rho^{\wedge}(\mathbb{Z}_n, m, 3) < n$, then $n = 3p$.

First, note that $m = \chi(\mathbb{Z}_n, 3)$, so $u(n, m, 3) = n$ and thus $u(n, m+1, 3) = n$ as well. Thus, looking at the conjectured formula for $\rho^{\wedge}(\mathbb{Z}_n, m, 3)$, to prove statement A, it suffices to verify that

A.1: $3(m+1) - 3 - \gcd(n, (m+1) - 1) \geq n$;

A.2: $3(m+1) - 9 \geq n$; and

A.3: If $3(m+1) - 10 < n$, then $\gcd(n, (m+1) - 1) \neq 7$, $m+1$ is not divisible by 3, and $(m+1) - 3$ is not divisible by 5.

Observe that if d divides both n and m , then d divides $3m - n$ as well, and so

$$\gcd(n, m) \leq 3m - n = n/p + 3,$$

which implies that

$$3(m+1) - 3 - \gcd(n, (m+1) - 1) \geq (p+1) \cdot n/p + 3 - (n/p + 3) = n,$$

proving A.1.

To prove A.2, observe that, since n is neither prime nor even, we have $n \geq 3p$, and so

$$3(m+1) - 9 = (p+1) \cdot n/p - 3 \geq n.$$

Similarly, we see that $3(m+1) - 10 < n$ may only occur if $n = 3p$, in which case $m = p+2$, but then neither 3 nor p divides m , so $\gcd(n, m) = 1$; $m+1 = p+3$ is not divisible by 3; furthermore, $m-2 = p$ is not divisible by 5 (since $p = 5$ would give $n = 15$, which we excluded). This proves A.3.

To prove statement B, we will suppose, indirectly, that $n \neq 3p$. But we assumed that n was odd and composite, so $n = 5p$ or $n \geq 7p$; furthermore, if $n = 5p$ then, for p to be the smallest prime divisor of n that is congruent to 2 mod 3, p would need to be 5. For $n = 25$ we get $m = 11$, but Conjecture 16 implies that $\rho^{\wedge}(\mathbb{Z}_{25}, 11, 3) = 25$, so we can rule out $n = 25$ and so assume that $n \geq 7p$. Thus, looking again at the conjectured formula for $\rho^{\wedge}(\mathbb{Z}_n, m, 3)$, to prove statement B, it suffices to verify that

B.1: $3m - 3 - \gcd(n, m - 1) \geq n$; and

B.2: If $n \geq 7p$, then $3m - 10 \geq n$.

The proofs of B.1 and B.2 are similar to that of A.1 and A.2, respectively—we omit the details. This completes the proof of statement B.

Assume now that n has no prime divisors congruent to 2 mod 3. This, of course, means that n itself is not congruent to 2 mod 3. We set

$$m = \left\lfloor \frac{n}{3} \right\rfloor + 3.$$

We need to prove that Conjecture 16 implies both of the following statements:

C: $\rho^{\wedge}(\mathbb{Z}_n, m+1, 3) = n$.

D: If $\rho^{\wedge}(\mathbb{Z}_n, m, 3) < n$, then n is divisible by 9.

This time we have $m = \chi(\mathbb{Z}_n, 3) + 2$, so $u(n, m, 3) = n$ and thus $u(n, m+1, 3) = n$ as well. Thus, looking at the conjectured formula for $\rho^{\wedge}(\mathbb{Z}_n, m, 3)$, to prove statement C, it suffices to verify that

C.1: $3(m+1) - 3 - \gcd(n, (m+1) - 1) \geq n$;

C.2: $3(m+1) - 10 \geq n$.

Suppose that d divides both n and m , then d divides

$$3m - n = \begin{cases} 9 & \text{if } n \equiv 0 \pmod{3}; \\ 8 & \text{if } n \equiv 1 \pmod{3}. \end{cases}$$

Therefore,

$$3(m+1) - 3 - \gcd(n, (m+1) - 1) \geq \begin{cases} n + 12 - 3 - 9 & \text{if } n \equiv 0 \pmod{3}; \\ n - 1 + 12 - 3 - 8 & \text{if } n \equiv 1 \pmod{3}. \end{cases}$$

This proves C.1. Since

$$m+1 \geq (n-1)/3 + 4,$$

statement C.2 follows as well.

To prove statement D, we first prove that $\gcd(n, m-1) \leq 5$. Indeed, if d is a divisor of both n and $m-1$, then d divides $3m-3-n$, which is at most 6; however d cannot be 6 as n is odd. We also see that

$$3m-8 \geq n-1+9-8 = n.$$

Furthermore, $m \neq 6$ since $n > 15$.

Therefore, according to Conjecture 16, for $\rho^{\wedge}(\mathbb{Z}_n, m, 3)$ to be less than n , we must have either n and m both divisible by 3, or n divisible by $3m-9$ and $m-3$ divisible by 5. Since in both these cases n is divisible by 3, we have $m = n/3 + 3$. We can rule out the second possibility: if $m-3 = n/3$ were to be divisible by 5, then n would be as well, contradicting our assumption that n has no prime divisors congruent to 2 mod 3. This leaves only one possibility: that n and m are both divisible by 3, which implies that n is divisible by 9, as claimed. Our proof of statement D and thus of Theorem 18 is now complete. \square

It is worth mentioning that, as a special case of Conjecture 17, for odd integers $n \geq 31$,

$$\chi^{\wedge}(\mathbb{Z}_n, 3) \leq \frac{2}{5}n + 1.$$

(The additive constant could be adjusted to include odd integers less than 31.) This conjecture was made by Gallardo, Grekos, et al. in [14], and (for large n) proved by Lev via the following more general result:

Theorem 19 (Lev; cf. [20]) *Let G be an abelian group of order n with*

$$n \geq 312|L| + 923,$$

where, as before, L is the collection of elements of G that have order at most 2. Then for any subset A of G , at least one of the following possibilities holds:

- $|A| \leq \frac{5}{13}n$;
- A is contained in a coset of an index-two subgroup of G ;
- A is contained in a union of two cosets of an index-five subgroup of G ; or
- $3^*A = G$.

So, in particular, if n is odd, is at least 1235, and a subset A of \mathbb{Z}_n has size more than $2n/5$, then the last possibility must hold, so we get:

Corollary 20 *If $n \geq 1235$ is an odd integer, then*

$$\chi^*(\mathbb{Z}_n, 3) \leq \frac{2}{5}n + 1.$$

The bound on n in Corollary 20 can hopefully be reduced.

As another special case of Conjecture 17, we claim that if $n \geq 83$ is odd and not divisible by five, then

$$\chi^*(\mathbb{Z}_n, 3) \leq \frac{4}{11}n + 1.$$

Theorem 19 does not quite yield this: while a careful read of [20] enables us to reduce the coefficient $5/13$ to $(3 - \sqrt{5})/2$ (at least for large enough n), this is still higher than $4/11$.

It is also worth pointing out that combining Theorem 9 with Conjecture 17 yields that, when $n \geq 11$, we have

$$\chi(\mathbb{Z}_n, 3) \leq \chi^*(\mathbb{Z}_n, 3) \leq \chi(\mathbb{Z}_n, 3) + 3.$$

This is in contrast to the fact that for every positive integer C , there are values of n and m so that the quantities $\rho^*(\mathbb{Z}_n, m, 3)$ and $\rho(\mathbb{Z}_n, m, 3)$ are further than C away from one another (cf. [4]).

Acknowledgments: The author acknowledges J. Butterworth's and K. Campbell's preliminary work on Theorems 8 and 9, respectively.

References

- [1] N. Alon, M. B. Nathanson, and I. Ruzsa, Adding Distinct Congruence Classes Modulo a Prime, *Amer. Math. Monthly*, **102** (1995) 250–255.
- [2] N. Alon, M. B. Nathanson, and I. Ruzsa, The Polynomial Method and Restricted Sums of Congruence Classes, *J. Number Theory*, **56** (1996) 404–417.
- [3] B. Bajnok, On the maximum size of a (k, l) -sum-free subset of an abelian group. *Int. J. Number Theory* **5**(6) (2009), 953–971.

- [4] B. Bajnok, On the minimum size of restricted sumsets in cyclic groups. To appear in *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.*; see also www.arxiv.org/pdf/1305.2141.
- [5] P. H. Diananda and H. P. Yap, Maximal sum-free sets of elements of finite groups. *Proceedings of the Japan Academy*, **45** (1969) 1–5.
- [6] J. A. Dias da Silva and Y. O. Hamidoune, Cyclic space for Grassmann derivatives and additive theory. *Bull. London Math. Soc.*, **26** (1994) 140–146.
- [7] G. T. Diderrich, An Addition Theorem for Abelian Groups of Order pq , *J. Number Theory*, **7** (1975) 33–48.
- [8] G. T. Diderrich and H. B. Mann, Combinatorial Problems in Finite Abelian Groups. *A Survey of Combinatorial Theory*, J. N. Srivastava et al., ed., North-Holland (1973).
- [9] S. Eliahou, M. Kervaire, and A. Plagne, Optimally small sumsets in finite abelian groups, *J. Number Theory*, **101** (2003) 338–348.
- [10] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*. L’Enseignement Mathématique, Geneva (1980).
- [11] P. Erdős and H. Heilbronn, On the addition of residue classes (mod p). *Acta Arith.*, **9** (1964) 149–159.
- [12] M. Freeze, W. Gao, and A. Geroldinger, The critical number of finite abelian groups. *J. Number Theory*, **129** (2009) 2766–2777.
- [13] M. Freeze, W. Gao, and A. Geroldinger, Corrigendum to “The critical number of finite abelian groups. *J. Number Theory*, **129** (2009) 2766–2777”, submitted to *J. Number Theory*.
- [14] L. Gallardo, G. Grekos, et al., Restricted addition in $\mathbb{Z}/n\mathbb{Z}$ and an application to the Erdős–Ginzburg–Ziv problem. *J. London Math. Soc. (2)*, **65** (2002) 513–523.
- [15] W. Gao and Y. O. Hamidoune, On additive bases. *Acta Arithmetica*, **88**:3 (1999) 233–237.
- [16] B. Girard, S. Griffiths, and Y. O. Hamidoune, k -sums in abelian groups. *Combin. Probab. Comput.*, **21**/4 (2012) 582–596.
- [17] J. R. Griggs, Spanning subset sums for Finite Abelian groups, *Discrete Mathematics*, **229** (2001) 89–99.
- [18] Y. O. Hamidoune and A. Plagne, A new critical pair theorem applied to sum-free sets in Abelian groups, *Comment. Math. Helv.*, **XX** (2003) 1–25.
- [19] Gy. Károlyi, A note on the Hopf–Stiefel function. *European J. Combin.*, **27** (2006) 1135–1137.
- [20] V. F. Lev, Three-fold Restricted Set Addition in Groups, *European J. Combin.* **23** (2002) 613–617.
- [21] H. B. Mann and Y. F. Wou, Addition theorem for the elementary abelian group of type (p, p) , *Monatshefte für Math.* **102** (1986) 273–308.
- [22] M. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. Graduate Texts in Mathematics **165**, Springer–Verlag (1996).

- [23] A. Plagne, Additive number theory sheds extra light on the Hopf–Stiefel \circ function, *Enseign. Math., II Sér.*, **49**:1–2 (2003) 109–116.
- [24] A. Plagne, Optimally small sumsets in groups, I. The supersmall sumset property, the $\mu_G^{(k)}$ and the $\nu_G^{(k)}$ functions, *Unif. Distrib. Theory*, **1** (2006), no. 1, 27–44.
- [25] D. Shapiro, Products of sums of squares, *Expo. Math.*, **2** (1984) 235–261.